Shelli Weisberg, Legislative Director
May 29, 2012
Committee on Energy and Technology

The ACLU of Michigan supports HB 5523. This bill would prohibit public and nonpublic institutions of education and higher education from requiring a student or applicant for admission to provide the institution with access to the student or applicant's personal internet or electronic accounts, and prohibit employers from requesting or requiring employees or applicants to disclose their user names or passwords to Internet sites and Web-based accounts as a condition of employment.

Many universities have recently started requiring student athletes to provide them with access to the private content on their social media accounts. Such was the case with defensive back Yuri Wright, a four-star recruit from Don Bosco Prep in New Jersey. The University of Michigan withdrew its scholarship offer to Wright when officials discovered racial and sexual slurs on his Twitter account[i]. Wright subsequently accepted a scholarship from the University of Colorado. Sometimes this is done by requiring student athletes to install social media spying software onto their personal electronic devices. Other times schools will require that friend them on Facebook or allow them to follow them on their private Twitter account. Some schools hire private companies to do this. A recent article in the Washington Post reported the following:

> *Schools are essentially paying for a software program that scans athletes' Tweets, Facebook posts and other social media activity 24 hours a day. The program zeroes in on keywords (popular ones include expletives, brands of alcohol, drinking games, opponents' names and common misspellings of racial profanities) and sends each athlete and coach or administrator an e-mail alert when a questionable post has been published. Coaches or administrators can log in with a username and password to see a list of student, and each student's "threat level" — green for low, orange for medium and red for high — and a link or screen shot of the comment that set off red flags.*

While students must agree to the terms of use and install applications allowing these companies to do so, if their school requires them to agree to these terms as a condition for playing on a particular team it is hardly done of free will or freely consented to.

This raises a number of concerning legal questions. By requiring students to friend a third party on Facebook, this may be a violation of the 4th amendment as an unreasonable search and seizure since students likely have a reasonable expectation of privacy if they have set their settings such that most information is to be kept private and only available to those they wish to have access.

In addition, monitoring the social media private accounts of students will likely lead to censorship of these accounts and this could violate the students' first amendment rights to freedom of speech. At least one federal circuit court has already held that Universities don't have the right to punish professors for what they state in their own publications. See Bauer v. Sampson, 261 F.3d 775 (9th Cir. 2001).

We believe that employer policies that request or require employees or applicants to disclose user names and/or passwords to their private internet or web-based accounts, or require individuals to let employers view their private content, constitute a frightening and illegal invasion of privacy for those applicants and employees -- as well those who communicate with them electronically via social media. While employers may permissibly incorporate some limited review of public internet postings into their background investigation procedures, review of password-protected materials overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications. As such, we believe that policies such as this are illegal under the federal Stored Communications Act (SCA), 18 U.S.C. §§2701-11[ii]. This law was enacted to ensure the confidentiality of electronic communications, and make it illegal for an employer or anyone else to access stored electronic communications without valid authorization. Additionally, such practices could arguably chill employee speech and due process rights protected under the First and Fourteenth Amendments to the U.S. Constitution[iii].

These types of practices also violate Facebook's own policies. Facebook's Statement of Rights and Responsibilities states under the "Registration and Account Security" section that Facebook users must make ten commitments to the company relating to the registration and maintenance of the security of the account. The Eighth Commitment states "You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account." https://www.facebook.com/terms#!/legal/terms. Thus, sharing one's

password or access to one's account with potential or current employers violates these terms of agreement.

Job applicants and employees should not have to give up their first amendment rights, as well as risk the security of their private information, by being forced to divulge their passwords to accounts in order to gain or maintain employment. We urge the committee members to support HB 5523.

---

[i] Services monitor athletes on Facebook, other sites: Kathleen Nelson knelson@post-dispatch.com, Wednesday, February 1, 2012

[ii] Section 2701 of the SCA makes it illegal to intentionally (1) access a facility through which an electronic communication service is provided, without valid authorization; or (2) exceed an authorization to access that facility, thereby obtaining an electronic communication while it is in electronic storage in such a system. 18 U.S.C. §2701(a)(1)-(2).

[iii] In a different context factually, the National Labor Relations Board (NLRB) made headlines last November by issuing a complaint against a Connecticut company that fired an employee who criticized the company on Facebook, in violation of the company's social media policy. E.g., "Feds: Woman Illegally Fired Over Facebook Remarks," available at: http://www.myfoxdc.com/dpp/news/offbeat/feds-woman-illegally-fired-over- facebook-remarks-110910?CMP=201011_emailshare; "Labor Board: Facebook Vent Against Supervisor Not Grounds for Firing," available at: http://www.cnn.com/2010/TECH/social.media/11/09/facebook.firing/index.html The NLRB maintains that both the firing and the social media policy itself violate employees' protected speech rights under the National Labor Relations Act. See NLRB Press Release, http://www.nlrb.gov/shared_files/Press%20Releases/2010/R-2794.pdf. While the Connecticut case involves the employee's right to engage in particular speech protected under the NLRA, it also addresses the limits that federal law places on employers' interference and monitoring of employees' social media use more generally, and thus is worthy of notice.